

11 December 2008

By: Lucian Constantin, Web News Editor



FBI's reputation  
exploited by online  
scammers  
U.S. Department of  
Justice

## **FBI Scam E-Mails Epidemic**

### *IC3 warns of new spam campaigns using the bureau's name*

Trying to benefit from the reputation and authority of certain government institutions is nothing new to online scammers. However, the Internet Crime Complaint Center (IC3) warns via a publicly available [intelligence note](#) that FBI officials in particular have found themselves at the center of several recent spam campaigns.

In their quest for increased fraudulent income, phishers will do almost anything, and they constantly prove innovative in their techniques. The ability to exploit the popularity of world events, organizations, or services to its fullest is a vital trait in their line of business, and the level of innovation in their techniques is what makes the fight against online fraud a constant cat-and-mouse game.

The latest scam involving the FBI that is currently in circulation is likely to originate in Nigeria, according to the IC3. The fake e-mails claim they represent an "official order" and, as usually, they focus around fake sums of money that individuals are supposedly entitled to. Nigerian fraudsters appear to be obsessed with concepts such as inheritance, which is constantly evoked in their scams.

According to the e-mails, the very important "order" comes from the fictional Anti-Terrorist and Monetary Crimes Division, which has blocked the transfer of the ridiculously large sum of money on the suspicion of being used to fund terrorist activities. In order to clear things up, the users are requested to submit their personal and banking information. The e-mails go even further and make threats of prosecution if the user does not comply.

To make the scam more believable, the e-mails claim that the order has been authorized by FBI's own Assistant Director, Kevin Favreau. This is a similar tactic, also seen in previous scams, one of which claimed to be from FBI's Deputy Director, John S. Pistole. "FBI Executives are briefed on numerous investigations, but do not personally contact consumers regarding such matters," warns the intelligence note. The IC3 notes that similar spam campaigns seen in 2008 targeted other governmental agencies such as the IRS, or even the IC3 themselves.

"The FBI does not send unsolicited e-mails of this nature. [•••] In addition, the IC3 does not send threatening letters to consumers demanding payments for Internet crimes," stresses the Center in its notification. "It is imperative consumers guard their PII [personally identifiable information]. Providing your PII will compromise your identity!" it adds.

This might sound like common sense to some of the more active Internet users, but make no mistake, there are enough people out there for these cyber crooks to prey on. In November, a Portland news agency covered the story of Janella Spears, a medical nurse who ended up paying a total of \$400,000 to Nigerian scammers in her obsession to get a long-promised inheritance. The [incredible story](#), which involved a series of fake e-mails claiming to be from President Bush, FBI Director Robert Mueller, the President of Nigeria, Bank of Nigeria and the United Nations, started with a payment of only \$100.